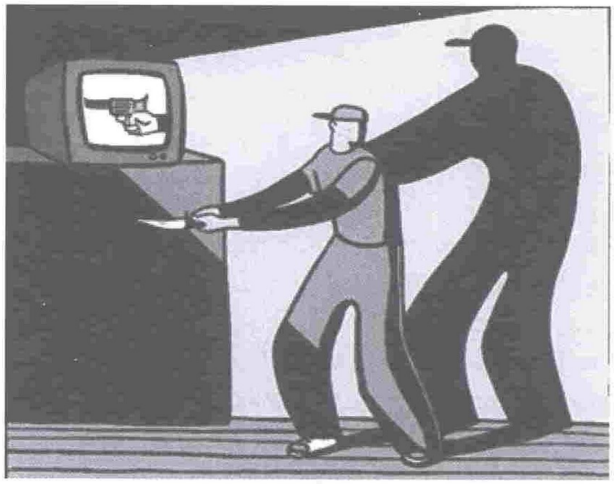
PROTECT Yourself

■ อุรุพจน์ กัลยาสิริ

ตรวจจับผู้บุกรุก : ความเสี่ยงของระบบคอมพิวเตอร์

ศึกษาความก้าวหน้าทางวิทยาการคอมพิวเตอร์ เพื่อนำมาประยุกต์ใช้กับการรักษาความปลอดภัยให้แก่ระบบ



วิทยาการด้านการรักษาความปลอดภัยให้แก่ระบบคอมพิวเตอร์ในเครือข่ายสื่อสารเป็นศาสตร์ที่เป็นที่สนใจกันมากในยุคปัจจุบัน อาจจะเป็นเหตุผลเนื่องมาจากความแพร่หลายของการใช้บริการผ่านเครือข่ายคอมพิวเตอร์หรืออินเทอร์เน็ตที่นับวันยิ่งมีมากขึ้น อัตราการเจริญเติบโตของเครือข่ายอินเทอร์เน็ตนับว่าเติบโตเร็วมาก จนในบางครั้งอาจเป็นจุดอ่อนสำคัญที่ทำให้ไม่มีความระมัดระวังหรือขาดการพิจารณาในการสร้างกฎเกณฑ์มาใช้ป้องกันความเสียหายที่จะเกิดขึ้นในอนาคต นับตั้งแต่อินเทอร์เน็ตเริ่มแพร่หลายเมื่อหลายปีก่อน มีผู้ไม่ประสงค์ดีได้สร้างความเสียหายมากมาย ทั้งที่ปรากฏเป็นข่าวใหญ่โตและทั้งที่ไม่ได้นำมาเปิดเผย ไม่ว่าเหตุการณ์นั้นจะถูกนำมาตีแผ่หรือไม่ก็ตาม ผู้ดูแลระบบเครือข่ายหรือผู้ดูแลระบบคอมพิวเตอร์ทั่วไปจำเป็นต้องติดตามข่าวสารต่าง ๆ เหล่านี้พร้อมทั้งควรศึกษาความก้าวหน้าทางวิทยาการคอมพิวเตอร์ เพื่อนำมาประยุกต์ใช้กับการรักษาความปลอดภัยให้แก่ระบบของตน หากผู้ดูแลระบบไม่มีความสนใจแล้ว กล่าวได้ว่าระบบนั้นมีความเสี่ยงต่อการบุกรุกจากผู้ไม่ประสงค์ดีเป็นอย่างยิ่ง

ข้อมูลที่เก็บรักษาไว้มีความสำคัญ

นับวันความต้องการที่จะปกป้องข้อมูลและการสร้างความปลอดภัยให้แก่ระบบคอมพิวเตอร์ในเครือข่ายยิ่งมีมากขึ้น อาจจะเป็นผลเนื่องมาจากข้อมูลที่ถูกเก็บรักษาเป็นข้อมูลที่มีความสำคัญมากขึ้น ทั้งในแง่ของการทำธุรกิจของภาคเอกชนทั่วไปและส่วนราชการ ข้อมูลที่จัดเก็บไว้ในระบบคอมพิวเตอร์สามารถจัดแบ่งได้เป็น 3 ชนิด

ชนิดแรกเป็นข้อมูลทั่วไปที่ต้องการบันทึกไว้เพื่อใช้ในการปฏิบัติงานหรือใช้ในการกำหนดนโยบายการดำเนินงาน ซึ่งโดยทั่วไปแล้วเป็นข้อมูลส่วนองค์กรที่ถูกจำกัดหรือไม่จำกัดการใช้ กล่าวคือ ข้อมูลบางส่วนไม่อนุญาตให้บุคคลทั่วไปเข้าถึงได้ แต่จะให้สิทธิ์เฉพาะพนักงานที่มีหน้าที่เท่านั้น ข้อมูลเหล่านี้ได้แก่ ประวัติพนักงานในองค์กร ข้อมูลลูกค้าหรือคนที่ต้องติดต่อกับองค์กร นโยบายการดำเนินงานขององค์กร ข้อมูลการเงินหรือข้อมูลความลับทางการค้า เป็นต้น หากเป็นองค์กรสำคัญก็จะมีการกำหนดสิทธิ์ที่เข้มงวดมากขึ้น เช่น นโยบายทางการเงินของราชการบางอย่างจะไม่อนุญาตให้บุคคลทั่วไปเข้าถึงได้ เป็นต้น ข้อมูลต่าง ๆ ที่กล่าวมานี้เป็นที่ต้องการของผู้ไม่ประสงค์ดีต่อองค์กร ซึ่งหากถูกโจรกรรมไปได้อาจจะมีผลต่อความมั่นคงขององค์กร และถ้าหากเป็นองค์กรที่มีความสำคัญระดับชาติแล้วก็จะยิ่งสร้างความเสียหายมากยิ่งขึ้นด้วย

ข้อมูลประเภทที่สองเป็นข้อมูลทางเทคนิคของระบบคอมพิวเตอร์นั้น ๆ เช่น แฟ้มข้อมูลในระบบคอมพิวเตอร์ที่ใช้กำหนดการทำงาน รหัสลับที่ใช้ในการเข้าถึงระบบคอมพิวเตอร์ ข้อมูลส่วนตัวของผู้ใช้ระบบในกรณีที่เป็นระบบเปิดอนุญาตให้มีผู้ใช้งานได้ โดยทั่วไปแล้วข้อมูลเหล่านี้เป็นที่ต้องการของผู้บุกรุกเนื่องจากเป็นข้อมูลสำหรับใช้ในการลักลอบเข้าสู่ระบบ ผู้บุกรุกจำเป็นต้องมีความรู้ทางด้านเทคนิคมากพอสมควร อาจจะอาศัยจุดอ่อนหรืออาศัยกระบวนการทำงานที่ไม่ปลอดภัยบางอย่างของมาตรฐานการสื่อสารข้อมูลก็ได้ การได้มาซึ่งข้อมูลเหล่านี้จะเป็นเสมือนประตูซึ่งเบิกทางสู่การโจรกรรมข้อมูลต่อไป แต่ก็มีผู้บุกรุกไม่น้อยที่ต้องการเพียงแค่เข้าสู่ระบบแล้วทำลายข้อมูลทางเทคนิคเหล่านี้เพียงอย่างเดียว นั่นก็เพียงเพื่อสร้างความเสียหายแก่ระบบนั่นเอง

ข้อมูลประเภทสุดท้ายเป็นข้อมูลที่ไม่มีความสำคัญใด ๆ ทั้งในแง่ที่เป็นความลับขององค์กรและทางด้านเทคนิค ซึ่งโดยทั่วไปแล้วผู้บุกรุกที่มีประสบการณ์จะสามารถแยกแยะได้และไม่สนใจกับข้อมูลประเภทนี้

http://www.sans.org/newlook/home.htm

การประยุกต์ใช้งานระบบเครือข่ายมีมากขึ้น

ผู้ดูแลเครือข่ายและระบบคอมพิวเตอร์มักจะเป็นนักวิชาการที่มีความรู้ทางด้านเทคนิคในการออกแบบและติดตั้งระบบคอมพิวเตอร์เพื่อใช้งานในองค์กร หรืออาจจะเป็นผู้ที่มีประสบการณ์ที่ทำงานเกี่ยวข้องทางเทคนิคมานาน ไม่ว่าจะเป็นบุคคลประเภทใดในบางครั้งอาจจะไม่สามารถทำให้ระบบเกิดความปลอดภัยมากที่สุดได้เนื่องจากเหตุผลหลาย ๆ ประการ เช่น ไม่มีความรู้ความสามารถเพียงพอที่จะออกแบบและจัดการ มีข้อจำกัดทางด้านการเงิน มีข้อจำกัดทางด้านเทคนิค หรือแม้กระทั่งเหตุผลด้านการบริหารงานในองค์กรเอง การประยุกต์ระบบให้สามารถทำงานได้ตามความต้องการขององค์กรนั้นเป็นปัจจัยสำคัญอีกอย่างที่เป็นตัวกำหนดให้ระบบมีความปลอดภัยที่จำกัด ตัวอย่างเช่น หากระบบมีการให้บริการหลายอย่างแก่ผู้ใช้จำนวนมาก และอยู่ในระบบเปิด (ระบบเปิดคือระบบที่สามารถเข้าถึงได้จากที่ใด ๆ ในเครือข่ายที่เชื่อมต่อกันด้วยมาตรฐานเดียวกัน) แล้ว ยิ่งเปิดโอกาสให้ผู้บุกรุกสามารถเข้าถึงได้ง่ายและสะดวกขึ้น มาตรการสร้างความปลอดภัยก็ทำได้ยากเนื่องจากต้องให้บริการแก่ผู้ใช้มากมาย โดยปกติแล้วจะไม่สามารถทราบได้โดยแน่ชัดว่าบุคคลที่ติดต่อเข้ามาขอใช้บริการนั้นประสงค์ดีหรือไม่ เพราะมีหลายครั้งที่ผู้ใช้บริการภายในที่มีสิทธิ์ถูกต้อง กลับกลายเป็นผู้บุกรุกเข้ามาทำลายระบบเสียเอง

ระบบที่ถูกจัดวางและติดตั้งในเครือข่ายคอมพิวเตอร์ในปัจจุบันแบ่งเป็น 2 ชนิดได้แก่ ระบบคอมพิวเตอร์ที่ให้บริการแก่ผู้ใช้ภายในองค์กร และอีกชนิดเป็นระบบที่เปิดให้บริการแก่บุคคลทั่วไปในเครือข่ายอินเทอร์เน็ต ระบบที่จัดบริการให้ผู้ใช้ภายในส่วนใหญ่จะให้บริการแก่ผู้ใช้งานที่มีหน้าที่ปฏิบัติงานอย่างใดอย่างหนึ่ง หรืออาจเป็นสวัสดิการให้แก่พนักงานในองค์กรก็ได้ ระบบนี้มีทั้งที่อนุญาตให้ใช้งานได้เฉพาะเครือข่ายภายในโดยไม่สามารถติดต่อสู่ภายนอกได้ กับแบบที่สามารถสร้างการเชื่อมต่อไปยังเครือข่ายอินเทอร์เน็ตภายนอกได้ หากเป็นระบบที่ให้ใช้ภายในเท่านั้นจะสามารถสร้างความปลอดภัยและกำหนดมาตรการรักษาความปลอดภัยได้ง่าย เนื่องจากจะทราบจำนวนและปริมาณการใช้งานที่แน่นอน และทั้งหมดก็อยู่ภายใต้การควบคุมขององค์กร หากมีการบุกรุกระบบก็สามารถติดตามและหาสาเหตุได้ง่าย หากระบบนั้นสามารถติดต่อสู่เครือข่ายอินเทอร์เน็ตภายนอกได้แล้วจะยิ่งมีความเสี่ยงมากขึ้น เนื่องจากอาจมีผู้ไม่ประสงค์ดีอาศัยช่องทางนี้เข้าสู่ระบบ ผู้ดูแลระบบจึงจำเป็นต้องกำหนดนโยบายการรักษาความปลอดภัยให้เข้มงวดมากขึ้น เพราะจะต้องระวังทั้งบุคคลภายในและภายนอกองค์กรที่มาจากเครือข่ายภายนอกด้วย

ระบบคอมพิวเตอร์แบบที่สองคือ ระบบที่ให้บริการแก่บุคคลทั่วไปในเครือข่ายอินเทอร์เน็ต ซึ่งโดยทั่วไปแล้วจะมีทั้งที่เป็นองค์กรที่ทำธุรกิจเพื่อแสวงหากำไรและองค์กรที่ให้บริการโดยไม่คิดมูลค่า ระบบที่ให้บริการเหล่านี้อาศัยลักษณะพิเศษของสถาปัตยกรรมเครือข่ายคอมพิวเตอร์ที่เปิดโอกาสให้สามารถเปิดบริการภายใต้มาตรฐานต่าง ๆ ในระบบเปิด กล่าวได้ว่าในสารบบของเครือข่ายคอมพิวเตอร์ มักจะอาศัยมาตรฐานระบบเปิดเดียวกันที่ใช้โปรโตคอลสื่อสารที่เรียกว่า ทีซีพี/ไอพี (TCP/IP : Transmission Control Protocol/Internet Protocol) นั่นเอง ทีซีพี/ไอพีเป็นชุดโปรโตคอลที่มีใช้กันอย่างแพร่หลายในระบบเครือข่ายอินเทอร์เน็ต เนื่องจากเป็นมาตรฐานที่สามารถปรับใช้ได้กับระบบทั่วไปจำนวนมากและเป็นมาตรฐานที่ถูกกำหนดขึ้นมาภายใต้ปรัญชาการเชื่อมต่อคอมพิวเตอร์และอุปกรณ์เครือข่ายให้เป็นระบบหนึ่งเดียวที่สามารถสื่อสารกันได้โดยไม่ขึ้นอยู่กับชนิดของฮาร์ดแวร์หรือระบบปฏิบัติการ บริการที่มักให้บริการกันได้แก่ การให้บริการเว็บ (WWW : World Wide Web) ดีเอ็นเอส (DNS : Domain Name System) จดหมายอิเล็กทรอนิกส์ (E-mail : Electronic Mail) กระดานข่าว (Bulletin Board) การโอนถ่ายแฟ้มข้อมูล (FTP : File Transfer Protocol) และอื่น ๆ อีกหลากหลายชนิด บริการเหล่านี้เปิดให้สามารถเรียกใช้ได้โดยง่ายเพียงแต่ผู้ใช้จะต้องเชื่อมต่อเข้าสู่เครือข่ายอินเทอร์เน็ต ด้วยจุดอ่อนที่เป็นระบบเปิดและข้อผิดพลาดบางประการของซอฟต์แวร์มักจะเป็นสาเหตุหลักที่ทำให้เกิดการบุกรุกเข้ามาสร้างความเสียหายให้แก่ระบบ

ความเสียหายที่เกิดขึ้นมีหลายสาเหตุ

หากจะแบ่งประเภทของการบุกรุกนั้นก็สามารถแบ่งได้หลายแบบ ซึ่งขึ้นอยู่กับเกณฑ์การจัดแบ่ง ถ้าพิจารณาการบุกรุกเข้ามาของผู้ไม่ประสงค์ดีต่อระบบโดยรวมแล้วสามารถแบ่งได้เป็น 5 ประเภท (จาก seminal report เรื่อง Computer Security Threat Monitoring and Surveillance โดย James P. Anderson ปี ค.ศ. 1980) ดังต่อไปนี้

http://www.cert.org/

ลวง (Masquerading)

จะใช้วิธีการทำให้ระบบเชื่อว่าการเข้ามาของผู้บุกรุกนั้นเป็นการเรียกใช้งานที่ถูกต้องและได้รับอนุญาตแล้ว เช่น การทำแอดเดรสลวง การส่งคำร้องขอลวง เป็นต้น เมื่อผู้บุกรุกสามารถลวงได้แล้ว จะเข้าสู่ระบบและสร้างความเสียหายต่าง ๆ

ดอส (DOS : Denial of Service)

เป็นวิธีที่นิยมใช้กับจุดอ่อนต่าง ๆ ของระบบปฏิบัติการคอมพิวเตอร์ และข้อบกพร่องของโปรแกรมให้บริการต่าง ๆ ของเซิร์ฟเวอร์เพื่อให้ระบบไม่สามารถให้บริการได้ตามปกติ โดยระบบมักจะมีทรัพยากรไม่เพียงพอต่อการให้บริการตามปกติ นอกจากนี้อาจทำงานผิดพลาดหรือบางครั้งอาจหยุดทำงานได้ เช่น การบุกรุกทางจุดอ่อนของบริการพื้นฐาน จุดผิดพลาดเนื่องมาจากการออกแบบระบบปฏิบัติการและโปรโตคอลที่ไม่รัดกุม

ใช้ทรัพยากรโดยไม่ได้รับอนุญาต (Unauthorized use of resources)

ผู้บุกรุกจะเข้าสู่ระบบแล้วรันโปรแกรมหรือเข้าใช้ทรัพยากรใด ๆ ของระบบที่ไม่ได้รับอนุญาตจนอาจมีผลทำให้ผู้ใช้คนอื่นไม่สามารถเข้าใช้ระบบได้ หรือใช้ทรัพยากรของระบบจนหมด หรือแม้กระทั่งทำให้ระบบโดยรวมเกิดความเสียหาย

โจรกรรมข้อมูล (Unauthorized disclosure of information)

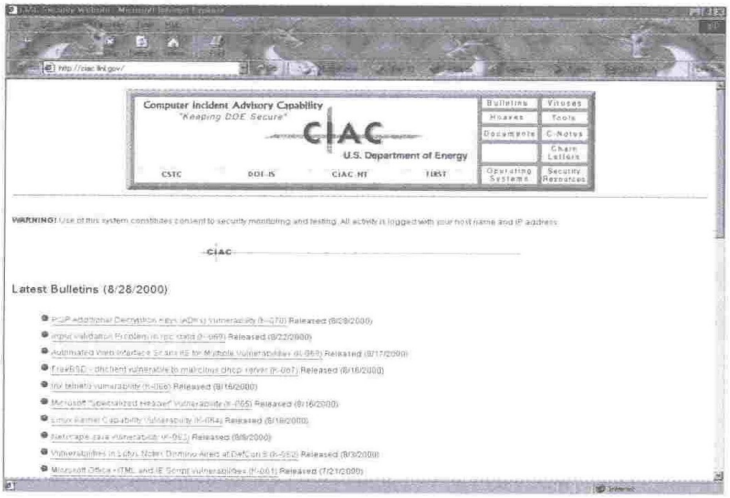
ผู้บุกรุกอาจเข้ามาโจรกรรมข้อมูลโดยการคัดลอกหรือถ่ายโอนข้อมูลความลับต่าง ๆ เช่น รหัสลับบัตรเครดิต ข้อมูลทางการค้าในกรณีที่เป็นองค์กรธุรกิจ ข้อมูลทางการทหารหากเป็นองค์กรทางการทหารหรือองค์กรที่มีหน้าที่รักษาความปลอดภัย

เปลี่ยนแปลงข้อมูล (Unauthorized alteration of information)

ข้อมูลอาจถูกเปลี่ยนแปลง โดยการเพิ่มเติม ลบทิ้งหรือถูกดัดแปลง ทำให้ผิดพลาดไปจากความถูกต้องของข้อมูลเดิม

ป้องกันความเสียหายที่จะเกิดขึ้น

โดยทั่วไปการป้องกันการบุกรุกเครือข่ายหรือระบบคอมพิวเตอร์แบ่งเป็น 2 วิธีคือ การป้องกันหรือตรวจจับก่อนเข้าสู่ระบบ อีกวิธีคือการป้องกันหรือสร้างความปลอดภัยให้โฮสต์ หากจะเปรียบเทียบให้บ้านคือระบบคอมพิวเตอร์ ส่วนผู้บุกรุกคือโจรแล้ว การป้องกันไม่ให้มีการโจรกรรมทรัพย์สินในบ้านก็เปรียบเสมือนการป้องกันไม่ให้เกิดการบุกรุกระบบคอมพิวเตอร์นั่นเอง หากกล่าวให้เข้าใจโดยง่ายจะเปรียบเทียบการป้องกันการโจรกรรมของโจรได้ 2 วิธีคือ วิธีแรกเป็นการจ้างเจ้าหน้าที่รักษาความปลอดภัยให้มาเฝ้าดูและตรวจตราหน้าบ้านมิให้บุคคลที่ไม่ได้รับอนุญาตเข้ามาในบ้านได้ ส่วนอีกวิธีคือการปิดประตูและหน้าต่าง ซ่อมแซมจุดบกพร่องหรือช่องทางที่จะเข้าสู่บ้าน ไม่ให้โจรสามารถใช้ช่องทางเหล่านั้นเข้าสู่บ้านได้ ระบบคอมพิวเตอร์ก็เช่นเดียวกัน การป้องกันวิธีแรกซึ่งมักจะทำกัน ได้แก่ การหาระบบป้องกันมิให้บุคคลที่ไม่ได้รับอนุญาตเข้าสู่ระบบได้ การสร้างนโยบายรักษาความปลอดภัยให้แก่เครือข่ายคอมพิวเตอร์ การติดตามหรือตรวจจับเหตุการณ์ที่น่าสงสัย ส่วนวิธีการป้องกันโฮสต์ ได้แก่ การตรวจดูความปลอดภัยของบริการต่าง ๆ ที่ระบบมีให้บริการว่าจะมีจุดบกพร่องจนอาจเป็นผลทำให้ผู้บุกรุกสามารถใช้จุดอ่อนเหล่านั้นและเข้ามาทำลายระบบได้ หรืออาจจะเป็นการเพิ่มความปลอดภัยให้แก่ระบบทั้งบริการต่าง ๆ และจุดบกพร่องของระบบปฏิบัติการเอง จะเห็นได้ว่าผู้ดูแลระบบควรป้องกันทั้งวิธีแรกและวิธีที่สองไปพร้อม ๆ กัน เพื่อให้ได้ผลที่มีประสิทธิภาพสูงสุด



http://ciac.llnl.gov/

นอกจากวิธีการป้องกันดังกล่าวแล้ว สิ่งสำคัญอีกอย่างคือ ผู้ดูแลระบบควรมีความรู้กว้างขวางในเรื่องการดูแลและจัดการระบบและเครือข่ายให้มีความปลอดภัยมากที่สุด สำหรับองค์กรที่ให้ความสำคัญกับการรักษาความปลอดภัยมากและมีงบประมาณที่เพียงพอมักจะว่าจ้างที่ปรึกษาให้จัดการเรื่องนี้ให้ซึ่งก็จะแก้ปัญหาส่วนใหญ่ไปได้ดี แต่หากองค์กรนั้นต้องการป้องกันข้อมูลความลับบางอย่างไม่ให้บุคคลภายนอกรู้ การใช้วิธีการว่าจ้างที่ปรึกษานี้ก็อาจทำให้ข้อมูลความลับเหล่านั้นถูกเปิดเผยได้ ในกรณีที่ผู้รับจ้างเป็นที่ปรึกษานั้นไม่มีจรรยาบรรณในการปฏิบัติงาน ดังนั้นก่อนการว่าจ้างให้ทำงานจะต้องมีข้อตกลงหรือสัญญาที่ชัดเจน เพื่อทำความเข้าใจก่อนการปฏิบัติงาน หากองค์กรใดไม่มีงบประมาณเพียงพอสำหรับว่าจ้างที่ปรึกษา หน้าที่ต่าง ๆ เหล่านี้จะตกเป็นของผู้ดูแลระบบเสียเป็นส่วนใหญ่ ดังนั้นผู้ที่รับผิดชอบเหล่านี้จึงควรหาความรู้ที่เกี่ยวข้องให้มากที่สุด แหล่งข้อมูลเหล่านี้สามารถค้นหาและศึกษาเพิ่มเติมได้จากเว็บต่าง ๆ เช่น

http://www.sans.org/newlook/home.htm
http://www.cert.org/
http://ciac.llnl.gov/

สรุป

โดยปกติแล้วเครื่องมือต่าง ๆ ที่ถูกพัฒนาขึ้นเพื่อจัดการเรื่องความปลอดภัยของระบบคอมพิวเตอร์นั้นมักถูกออกแบบขึ้นเพื่อป้องกันการบุกรุกผ่านบริการที่มีจุดบกพร่องต่าง ๆ หรือเหตุการณ์ที่มักเกิดขึ้นอยู่เสมอ ๆ ซึ่งสามารถป้องกันได้เพียงบางส่วนเท่านั้น ดังนั้นสิ่งที่ผู้ดูแลระบบควรตระหนักเป็นอย่างยิ่งก็คือ การเปิดให้บริการใด ๆ ก็ตามที่มักมีปัญหาทำให้ระบบทำงานช้าหรือเปลืองทรัพยากรมากก็ไม่ควรทำ และหากทราบว่ามีจุดบกพร่องใด ๆ เกิดขึ้นกับบริการใดก็ควรงดการให้บริการนั้น ๆ ทันทีเพื่อป้องกันไม่ให้เกิดความเสียหายต่อไป